

COMMUNITY SECURITY BLUEPRINT

Protect your people. Defend your community. Deter, detect, respond.

3 Layers

defense in depth

24/7

watch rotation

Community

strength in numbers

Non-lethal

first line always

WHAT'S INSIDE:

- 1 Threat Assessment
- 3 Watch & Patrol Systems
- 5 Conflict De-escalation
- 7 Community Security Network

- 2 Perimeter & Detection
- 4 Communication Protocols
- 6 Non-Lethal Defense
- 8 Quick Reference Card

You cannot defend against everything. Identify your actual threats and plan accordingly.

Security without threat assessment wastes resources defending the wrong things. The most dangerous threats change over time. Reassess regularly and adjust your posture.

THREAT CATEGORIES

OPPORTUNISTIC CRIME

RISK: HIGH

Individuals taking advantage of reduced law enforcement or desperate conditions.

- Unlocked doors, unguarded supplies, visible valuables
- Mitigated by: visible security, locks, lighting, community presence

ORGANIZED GROUPS

RISK: MEDIUM-HIGH

Small organized groups seeking food, supplies, or territory by force.

- Target isolated or undefended households
- Mitigated by: community coordination, perimeter, early warning

INFORMATION THREATS

RISK: MEDIUM

People gathering intelligence on your resources for later exploitation.

- Strangers asking too many questions, unusual surveillance
- Mitigated by: information discipline, need-to-know policy

INTERNAL CONFLICT

RISK: MEDIUM

Disputes within the community over resources, roles, or decisions.

- Unaddressed grievances, resource inequality, power struggles
- Mitigated by: clear governance, fair distribution, conflict resolution

NATURAL/ENVIRONMENTAL

RISK: VARIABLE

Fire, flood, animal threats, or other natural hazards affecting security.

- Depends heavily on location and season
- Mitigated by: early warning systems, evacuation planning

VULNERABILITY ASSESSMENT

Ask these questions about your location:

PHYSICAL VULNERABILITIES

- Easy entry points: gaps in fences, unlocked doors
- Poor lighting around perimeter at night
- No natural barriers (walls, fences, water, terrain)
- Single entry/exit point with no alternate escape route
- Valuables visible from road or neighboring properties

INFORMATIONAL VULNERABILITIES

- Community members discussing resources publicly
- No information sharing policy — everyone knows everything
- Outsiders know your supply levels or group size
- Predictable schedules and routines (easy to plan against)
- No vetting process for new members or visitors

OPERATIONAL VULNERABILITIES

- No watch rotation — gaps in monitoring
- No alarm or early warning system in place
- No communication plan if threat occurs
- No designated roles during an incident
- No plan for medical response during security incident

THREAT LEVEL SYSTEM

GREEN — NORMAL

Routine operations. Standard watch. No known threats.

AMBER — ELEVATED

Increased awareness. Double watch at night. Limit outsider access.

ORANGE — HIGH

Active threat nearby. All posts manned. No solo movement.

RED — CRITICAL

Immediate threat. Full lockdown. All members to positions.

Defense in depth: three layers that each slow, detect, or deter threats.

No single barrier stops a determined threat. Your goal is to slow intruders, detect them early, and buy time for your community to respond. Each layer adds cost and delay for an attacker.

LAYER 1 — OUTER PERIMETER

Early Warning Zone (100–300 metres out)

Purpose: Detect approaching threats **BEFORE** they reach your position.

- **Natural observation points:** High ground, corners, choke points with clear sightlines.
- **Early warning devices:** Trip lines with noise makers (cans, bells), motion-sensitive alarms.
- **Signage and deterrence:** Visible 'Community Watch Active' signs deter casual opportunists.
- **Patrol routes:** Irregular patrol patterns covering the outer perimeter.

LAYER 2 — BOUNDARY

Physical Barrier (immediate property edge)

Purpose: Channel entry through controlled points. **Slow and funnel intruders.**

- **Fencing and walls:** Chain link, wooden fence, thorny hedges, wire. Imperfect is fine — it slows.
- **Controlled entry:** Single or double entry point with someone present at all times during threat.
- **Barrier reinforcement:** Stack debris, vehicles, or materials to block weak points temporarily.
- **Lighting:** Motion-activated or continuous lighting at all entry points and corners.

LAYER 3 — INNER DEFENSE

Core Living/Storage Area

Purpose: Final hardened position if outer layers fail.

- **Hardened safe room:** One room reinforced as last refuge. Solid door, reinforced frame.
- **Supply storage:** Critical supplies inside inner layer — not accessible from outside.
- **Communication post:** Radio/signaling equipment in inner layer for calling outside help.
- **Escape route:** At least one planned secondary exit from inner position.

KEY PRINCIPLE:

Perimeter security does not have to be perfect — it has to be better than your neighbors. Opportunistic threats choose the easiest target. Visible deterrence redirects most threats elsewhere.

A watch system is your most important security tool — more than any physical barrier. No fence stops a threat that has not been detected. Early warning gives your community time to respond, deter, or evacuate. A well-organized watch system costs nothing but time.

WATCH ROTATION DESIGN

Time	Watch A	Watch B	Watch C
06:00–12:00	Day 1	Day 2	Day 3
12:00–18:00	Day 4	Day 5	Day 6
18:00–00:00	Day 2+3	Day 4+5	Day 6+1
00:00–06:00	Day 5+6	Day 6+1	Day 2+3

WATCH POST REQUIREMENTS

- Position:** Elevated or covered vantage point with 180°+ sightline.
- Equipment:** Binoculars, flashlight, watch/timepiece, communication device.
- Log book:** Record: time, weather, observations, any incidents.
- Comfort:** Weather protection — exhausted watchers miss threats.
- Check-in:** Radio/signal check with base every 30 minutes.
- Buddy system:** Never solo post at night. Two watchers minimum after dark.

PATROL PROTOCOLS

- VARY YOUR ROUTES**
Never patrol the same route twice in a row. Predictable patrols are easily avoided by threats.
- PATROL IN PAIRS**
Solo patrol is dangerous. Pairs can cover each other, deter confrontation, and get help if needed.
- SILENT MOVEMENT**
At night, move quietly. Talk in low voices. Use pre-agreed hand signals. Noise gives away position.
- OBSERVE, DON'T ENGAGE**
The job of patrol is intelligence gathering. Report threats — don't confront alone.
- PRE-ARRANGED SIGNALS**
Establish: one whistle = all clear, two = report in, three = alert, horn/bell = full emergency.
- EMERGENCY PROTOCOL**
If patrol encounters a threat: do NOT engage. Fall back, signal alarm, report position and description.

INCIDENT LOG FORMAT

Date & Time:

Location:

Description:

Action Taken:

Reported To:

Follow-up Required:

A security team that cannot communicate cannot coordinate. Plan this before you need it.

COMMUNICATION HIERARCHY

PRIMARY: Two-Way Radio

- FRS/GMRS radios: inexpensive, 1–5km range.
- Assign dedicated channel for security comms only.
- Keep radios charged. Have backup batteries.
- Encrypt channel: use code words for sensitive info.

SECONDARY: Physical Messenger

- Designated runner between posts if radio fails.
- Pre-set routes and timing for message runs.
- Use written messages for complex information.
- Never carry sensitive information without need.

EMERGENCY: Audible Signals

- Horn, bell, or whistle signals the whole community.
- Pre-agree: 1 blast = check in, 3 blasts = emergency.
- Practice signal recognition monthly.
- Position signal source centrally for maximum range.

BACKUP: Visual Signals

- Mirror flash, colored flags, or light signals.
- Use for day communication when noise is risk.
- Pre-agree a signal chart and post it at each station.
- Smoke signals for long-range daytime emergencies.

CODE WORD SYSTEM

Create your own code words. Example system:

- EAGLE:** All clear, situation normal
FALCON: Unknown person at perimeter
HAWK: Threat confirmed — all respond
NEST: Return to base immediately
MIGRATE: Execute evacuation plan

CRITICAL:

Never discuss watch schedules, supply locations, or group size on open radio. Assume any radio transmission can be monitored.

RESPONSE PROTOCOLS

UNKNOWN PERSON AT PERIMETER

- 1. Two people approach from different angles — never alone.
- 2. Maintain 10+ metre distance initially.
- 3. Ask purpose of visit, destination, and whether expected.
- 4. Offer to escort — never allow unsupervised access.
- 5. Log name, description, time, and stated purpose.

HOSTILE INDIVIDUAL

- 1. Alert all watch posts immediately via radio.
- 2. Increase distance. Do not engage physically.
- 3. Display group presence — more people visible = deterrent.
- 4. Clear bystanders to safety without creating panic.
- 5. Give clear, calm instruction to leave. Log and monitor.

MULTIPLE INTRUDERS / ORGANIZED THREAT

- 1. Sound emergency signal immediately.
- 2. All non-security members to inner safe area.
- 3. Security team to pre-assigned positions — do not cluster.
- 4. Assess numbers and direction. Report, do not engage solo.
- 5. Attempt to negotiate distance. Overwhelming presence deters.

DE-ESCALATION FIRST:

Physical confrontation should always be the last resort. Most threats will disengage when faced with an organized, visible, calm community response.

SECTIONS 5 & 6 — DE-ESCALATION & NON-LETHAL DEFENSE Resolve Without Violence

DE-ESCALATION PRINCIPLES

Why this matters:

Violence escalates situations, creates enemies, depletes resources, causes injuries, and attracts more conflict. The goal is always to resolve threats without physical confrontation.

STAY CALM

Your calm projects competence and control. Fear or aggression from you escalates the other person. Take a breath. Slow your voice. Stand tall but relaxed.

LISTEN FIRST

Most conflicts begin with someone feeling unheard. Let the person speak. Understand their actual need before responding. Often people want acknowledgment, not resources.

SHOW NUMBERS, NOT AGGRESSION

Have multiple people visible. A crowd that is calm but present says: we are organized. This deters more effectively than a single person acting aggressively.

OFFER A SMALL WIN

Where possible, give something minor: information, directions, water, a moment of time. People who get something are far less likely to escalate.

GIVE A CLEAR EXIT

Always give the other party a way to leave without losing face. Backed-into-corner situations escalate. An easy exit is used.

WHEN TO STOP TRYING

If weapons are displayed, threats become specific, or the person is clearly irrational: stop negotiating. Withdraw, create distance, signal alarm, wait for backup.

NON-LETHAL DEFENSE OPTIONS

Use in order — start with deterrence, escalate only if needed:

1. VISIBLE PRESENCE

Numbers

- Multiple people visible at perimeter.
- High-visibility vests or clothing.
- Active and visible patrol movements.
- Calm, organized, purposeful behavior.

2. BARRIERS & OBSTACLES

Physical

- Locked gates and reinforced entry points.
- Vehicles positioned to block vehicle access.
- Thorny hedges or wire at perimeter gaps.
- Bright lighting directed at approach routes.

3. NOISE & ALARMS

Deterrence

- Air horns or whistles on patrol.
- Trip wire alarms at perimeter gaps.
- Dogs — highly effective deterrent.
- Vehicle horn as community alarm signal.

4. CHEMICAL DETERRENTS

Last non-lethal resort

- Pepper spray / OC spray — legal in most places.
- Only used in direct close-range threat.
- Carrier wind direction before use.
- Effective range: 3–5 metres.

5. IMPACT DETERRENTS

Close-range only

- Batons or sticks as last resort deterrents.
- Purpose is to create pain compliance, not injury.
- Requires training to use effectively.
- Always outnumber the threat before engaging.

LEGAL NOTE:

Laws on self-defense and use of force vary by location. Know your local laws. Document all incidents immediately. The goal is always to avoid injury to all parties.

A coordinated neighborhood is exponentially more secure than isolated households.

Individual household security has hard limits. A network of households with clear roles, shared information, and coordinated response provides mutual protection that no single group can achieve alone.

THE FIVE HOUSEHOLD SECURITY NETWORK

HH 1 COMMAND	Security coordinator. Maintains threat log. Calls threat level changes. Coordinates response to all incidents. Maintains communication with all posts.
HH 2 EARLY WARNING	Outer perimeter monitoring. Manages trip wire and alarm systems. First notification when unknown persons approach. Provides threat description to Command.
HH 3 PATROL	Foot patrol responsibility for perimeter and common areas. Manages watch rotation schedule. Maintains patrol logs and incident reports.
HH 4 COMMUNICATIONS	Maintains all radios and communication equipment. Manages code word list. Relay station if direct communication fails. Contacts outside help if needed.
HH 5 SANCTUARY	Designated safe refuge for non-security members during incidents. Maintains inner defense position and supply security. Medical response capability.

MUTUAL AID AGREEMENTS

INFORMATION SHARING RULES

- Share threat intelligence immediately — timing matters.
- Do NOT share: supply quantities, group size, or internal conflicts.
- Use code words for radio communication of sensitive details.
- Debrief after every incident within 24 hours.
- Maintain a shared threat log accessible to all household leads.
- Monthly security meeting: reassess threats, update protocols.

Respond to emergency signals All households respond to three-blast alarm within 5 minutes.
Share threat intelligence Any household observing a threat notifies all others immediately.
Resource sharing in crisis Pre-agree which resources are shared and under what conditions
Non-combatant protection Designated safe house for children, elderly, and injured.
Post-incident review All incidents reviewed collectively. Lessons applied.

Critical information at a glance.

SIGNAL CODES

1 whistle/horn All clear — check in	2 whistles Report to base	3 whistles ALERT — all respond	Continuous horn EMERGENCY — full lockdown
---	-------------------------------------	--	---

THREAT LEVELS

GREEN Normal Standard watch. Routine ops.	AMBER Elevated Double night watch. Limit access.	ORANGE High All posts manned. No solo movement.	RED Critical Full lockdown. All to positions.
---	--	---	---

WATCH POST CHECKLIST

- ☐ Radio charged and tested
- ☐ Log book and pen present
- ☐ Flashlight working
- ☐ Binoculars at post
- ☐ Check-in schedule confirmed
- ☐ Buddy present (night posts)
- ☐ Emergency signal practiced
- ☐ Incident log from last shift reviewed

UNKNOWN PERSON RESPONSE

- Alert all posts via radio
- Approach in pairs — maintain 10m distance
- Ask: purpose, destination, who they know here
- Offer escort — no unsupervised access
- Log: time, description, stated purpose
- Monitor for 30 min after departure

DE-ESCALATION QUICK STEPS

Stay calm Slow voice, relaxed stance, steady eye contact.	Listen Let them speak. Nod. Acknowledge their words.	Show numbers Have 3+ people visible. Calm, not aggressive.	Offer something Water, directions, a moment — small win reduces tension.	Give an exit Always leave them a way to leave without losing face.
---	--	--	--	--

AbzuNet Freedom Suite | SynthiSoft Labs LLC | Open Source — Copy, Share, Print, and Build Freely.

"Safety is not the absence of threat. It is the presence of community."